TESTIMONY OF

RICHARD C. LAMAGNA
SENIOR MANAGER, WORLDWIDE ANTI-PIRACY INVESTIGATIONS
LAW AND CORPORATE AFFAIRS
MICROSOFT CORPORATION

BEFORE THE
HOUSE SUBCOMMITTEE ON COURTS,
THE INTERNET, AND INTELLECTUAL PROPERTY

MARCH 13, 2003

THE GLOBAL THREAT OF SOFTWARE COUNTERFEITING

Mr. Chairman, members of the Subcommittee, thank you for the opportunity to testify on this important topic. My name is Rich LaMagna, and I am Senior Manager of Worldwide Anti-Piracy Investigations at Microsoft Corporation. I joined Microsoft in 1999 after a 28-year career as a Special Agent with the DEA and the FBI investigating international drug trafficking organizations. My testimony this morning will focus on software counterfeiting -- the illegal manufacture and sale of pirate CD-ROMs, packaging, and other physical components. This particularly sophisticated form of piracy is increasingly dominated by international organized crime groups that produce billions of dollars in counterfeit software each year.

I. The Scope and Impact of Software Counterfeiting

A. Economic Contribution of the Commercial Software Industry

Over the past 25 years, computer software has fundamentally reshaped every facet of our lives and helped secure this country's economic leadership. By the late 1990s, the software industry employed more than 800,000 U.S. workers with aggregate wages of $55.6 billion. By the year 2008, the software industry is expected to employ more than 1.3 million workers in the United States alone.

Annually, the software industry contributes more than $28 billion in tax revenues to federal and state governments, benefiting a host of national and community programs. This tax contribution is expected to reach $50 billion by the year 2008. Also significant is the industry's contribution to the U.S. balance of payments. While the U.S. trade deficit reached new record highs in 2000, the U.S. software industry generated a trade *surplus* of more than $20 billion. The software industry's growing trade surplus means more jobs and tax revenues for the U.S. economy.

The success of the U.S. software industry is due in large part to this country's historical commitment to strong intellectual property protection. It is no coincidence that the United States—the world's leading advocate for intellectual property rights—is also home to the world's largest software industry. The software industry's continued growth and economic contributions are directly dependent on our ability as an industry and a nation to eliminate software theft.

B. Economic Impact of Software Piracy and Counterfeiting

For almost fifteen years, the software industry has battled against software theft, recognizing that widespread piracy threatens the very existence of our industry. Despite these efforts, software piracy remains a serious problem throughout the world, accounting for one-quarter of the software used in the United States, and 40 percent of the software used worldwide. In parts of Asia and the former Soviet Republic, piracy rates approach 90 percent, virtually eliminating sales of legitimate software.

The software industry loses almost $11 billion each year from counterfeiting and other forms of software piracy. Annual seizures of counterfeit Microsoft products exceed $1.7

billion. These revenue losses directly translate into lost jobs and opportunities for the U.S. economy. By the late 1990's, software piracy had cost the U.S. economy more than 109,000 jobs and almost 1 billion in tax revenues; by 2008, piracy-related losses will nearly double, accounting for 175,000 lost jobs and $1.6 billion in lost tax revenues.

II. Trends in Software Counterfeiting Operations

Unlike the cheap fakes sold on street corners, counterfeit software is typically marketed as genuine product to unsuspecting consumers who would never knowingly purchase illegal products. To create the look of genuine packaged software, counterfeiters use state-of-the-art technology to create near-perfect copies of Microsoft CD-ROMs, packaging, documentation and other components. Because counterfeiters bear none of the R&D, marketing or support costs that determine the price of legitimate software, these criminal operations are able to reap enormous profits from the sale of counterfeits.

A. Trafficking in Physical Anti-counterfeiting Features

For many years, Microsoft has worked to outpace counterfeiting technology by developing physical product features that help consumers and law enforcement agencies distinguish legitimate software from sophisticated counterfeits, much in the same way the US Government authenticates its paper currency. For example, Microsoft packaging has for many years included a certificate of authenticity ("COA") that incorporates special inks, holograms and micro-text. Microsoft has invested several millions of dollars to develop an edge-to-edge hologram that covers the entire surface of the CD-ROM. (Examples of these features are included in Attachment to this testimony.) The edge-to-edge hologram involves a highly sophisticated, proprietary technology that is etched into recent versions of Microsoft Office.

Because these physical anti-counterfeiting features are increasingly difficult to reproduce, counterfeiters are now combining pirate CD-ROMs and packaging with genuine components obtained through theft or fraud. In recent years, more than 100 robberies of authorized replicators in the US and Europe have netted 540,000 Microsoft COAs with an estimated value of $50 million. According to our sources, genuine COAs, end user manuals, end user license agreements and other physical components are in high demand among counterfeiters because they significantly increase the marketability and selling price of counterfeit software.

So far, counterfeiters have found it impossible to replicate the edge-to-edge technology. As an alternative, they have developed holographic stickers that, when attached to the CD-ROM, closely resemble the look of the edge-to-edge hologram. Recent versions of these fake stickers found in Asia are of such high quality, few consumers would be able to detect the counterfeit.

B. Proposed Clarification to Federal Anti-counterfeiting Law

Currently, federal law prohibits trafficking in counterfeit software and "counterfeit labels," but does not provide adequate civil and criminal remedies to combat the sale of genuine physical components or the combination of stolen components with counterfeit CD-

ROMs and packaging. Moreover, it is unclear whether prohibitions against counterfeit labels would cover counterfeit edge-to-edge holograms or COAs. This loophole in existing federal law makes it very difficult for prosecutors to target those criminals who clearly facilitate counterfeit sales by trafficking in genuine or counterfeit physical anti-counterfeiting features.

Mr. Chairman, we thank you for your leadership last year in introducing a clarification to federal anti-counterfeiting law that would close this loophole. We look forward to the opportunity to work with you and the Subcommittee to address this matter.

III. Involvement of Organized Crime

The production and distribution of high quality counterfeit software require a high level of planning, funding and organization; and access to replicating equipment, raw materials, packaging, shipping facilities, and money laundering avenues. Because of the enormous opportunities for profits and the low risk of prosecution or significant punishment, software counterfeiting has become part of an intricate web of international organized crime. Although crime groups based in Asia produce the largest quantity of sophisticated counterfeits, manufacturing and distribution centers exist throughout the world. In fact, California is a major entry and assembly point for counterfeit software CD-ROMs and components.

.

The federal government explicitly acknowledged the growing involvement of organized crime when it created a new "Intellectual Property Rights Initiative" in 1999 to strengthen enforcement against intellectual property crime. At a congressional hearing, former Customs Commissioner Ray Kelly stated that—

> *Our investigations have shown that organized criminal groups are heavily involved in trademark counterfeiting and copyright piracy. They often use the proceeds obtained from these illicit activities to finance other, more violent crimes. These groups have operated with relative impunity. They have little fear of being caught—for good reason. If apprehended, they face minimal punishment. We must make them pay a heavier price.*

Global counterfeiting flourishes because counterfeiters face little risk of prosecution or meaningful punishment. In the United States, Microsoft and other intellectual property owners have worked closely with Congress and Federal authorities to ensure that counterfeiting laws, enforcement, and penalties keep pace with counterfeiting crimes. In recent years, these efforts have led to important reforms, including improved sentencing guidelines for intellectual property crime, increased appropriations for IP-related law enforcement activities, and the creation of the FBI Cyber Division.

In addition, Microsoft invests millions of dollars each year to assist law enforcement in investigating criminal counterfeiting operations. Microsoft's worldwide anti-piracy team consists of more than 100 attorneys, forensic experts, and in-house and outside investigators, who work closely with law enforcement agencies in this country and throughout the world to investigate and prosecute international networks of criminal counterfeiters. In the United States, Microsoft's investigative team has worked closely with Federal and local law

enforcement to bring about important counterfeiting seizures, a number of which involved organized crime:

- In February 2000, the FBI and LA Sheriff's Office led 12 raids against suspected criminal counterfeiters, resulting in the arrest of 12 individuals. Law enforcement officials seized several thousand counterfeit copies of Microsoft software, worth more than $5 million. The persons arrested were part of a well-organized international counterfeiting operation, with ties to organized crime groups based in Asia.

- In November 2001, the LA Sheriff's office, aided by U.S. Customs, the Secret Service and Microsoft investigators, executed the most significant raid and seizure of Microsoft software and components in U.S. history, with an estimated retail value of $100 million. The raid interrupted a major counterfeit software distribution pipeline that moved containers of counterfeit software and other illegal components from Taiwan through the Port of Los Angeles. Taiwan authorities later confirmed that the counterfeiting operation was financed by criminal groups based in Asia.

- In April 2002, the FBI and several other federal and local law enforcement agencies dismantled a highly organized international counterfeiting ring, with assembly and distribution arms in Northern California, Washington and Oregon and direct ties to Asia-based criminal groups. The undercover investigation, known as "Operation Cyberstorm," led to the arrest of 27 individuals and the seizure of approximately $10 million in counterfeit software and components. The counterfeiters were also involved in money laundering and credit card fraud.

These cases demonstrate the critical importance of close, multilateral cooperation between industry and law enforcement. For example, in the 2001 raid described above, Taiwan authorities worked closely with US law enforcement and Microsoft to investigate and prosecute the leaders of the operation based in Asia. Unfortunately, few foreign law enforcement agencies share this commitment to anti-counterfeiting enforcement; and, as a result, the foreign criminals that finance and control worldwide counterfeiting operations are rarely prosecuted or punished.

In closing, we face a daunting challenge. How can we successfully fight a well-financed, global network of counterfeiting rings, when the criminals who control these operations bear little risk of prosecution and meaningful punishment outside the United States? Clearly, we cannot succeed, until all governments recognize that software counterfeiting is a serious crime that demands the same level of enforcement and cooperation that we bring to other global organized crime activities. We encourage Federal law enforcement agencies to join together in sending a clear, unified, and unequivocal message to foreign authorities that software counterfeiting is a major crime priority that demands tough penalties, a sustained commitment of law enforcement resources, and multilateral cooperation among national authorities and industry.

Thank you.

Attachment

Examples of Microsoft Anti-counterfeiting Features

Certificate of Authenticity

CD-ROM Edge-to-Edge Hologram